Software Safety Requirements and Architecture: Lane Assistance

Document version: 0.1

Template version: 1.0, Released on 2017-06-21

Author:
Konstantin Selyunin

August 28, 2018

Revision History

Version	Date	Editor	Description
0.1	2018/08/23	Konstantin Selyunin	LaTeX template created
0.2	2018/08/27	Konstantin Selyunin	Filling the content part

Contents

1 Purpose of the Software Safety Requirements and Architecture

ISO 26262 [1] suggests to use a V-model for the software product development lifecycle. The main steps of the **V** model for software development can be summarized as follows:

- Specification of software safety requirements
- Software architectural design
- Software unit design and implementation
- Software unit testing
- Software integration and testing
- Verification of software safety requirements

Software Safety Requirements come from Technical Safety Requirements, and in addition should cover the following:

- Maintaining or reaching a safe state
- Detecting, indicating, and handling software and hardwar faults

In order to facilitate ISO 26262 compliance of a software system, we need to approach software development systematically: i.e. first define the software requirements, then devise a software architecture, and then implement a system based on the pre-defined requirements and architecture.

2 Inputs to the Software Requirements and Architecture Document

2.1 Technical safety requirements

Technical Safety Requirements related to Functional Safety Requirement 01-01 are presented in Table 21

Table 21: Technical Safety Requirements for Functional Safety Requirement 01-01

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the **'Final electronic power steering Torque'** component is below Max_Torque_Amplitude	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-01-02	As soon as the LDW function deactivates the LDW feature, the **'LDW Safety'** software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	ignition cycle	**Memory Management Unit**	the lane assistance item is turned off

2.2 Refined Architecture Diagram from the Technical Safety Concept

The refined architecture of the lane assistance item is shown in Figure 21.

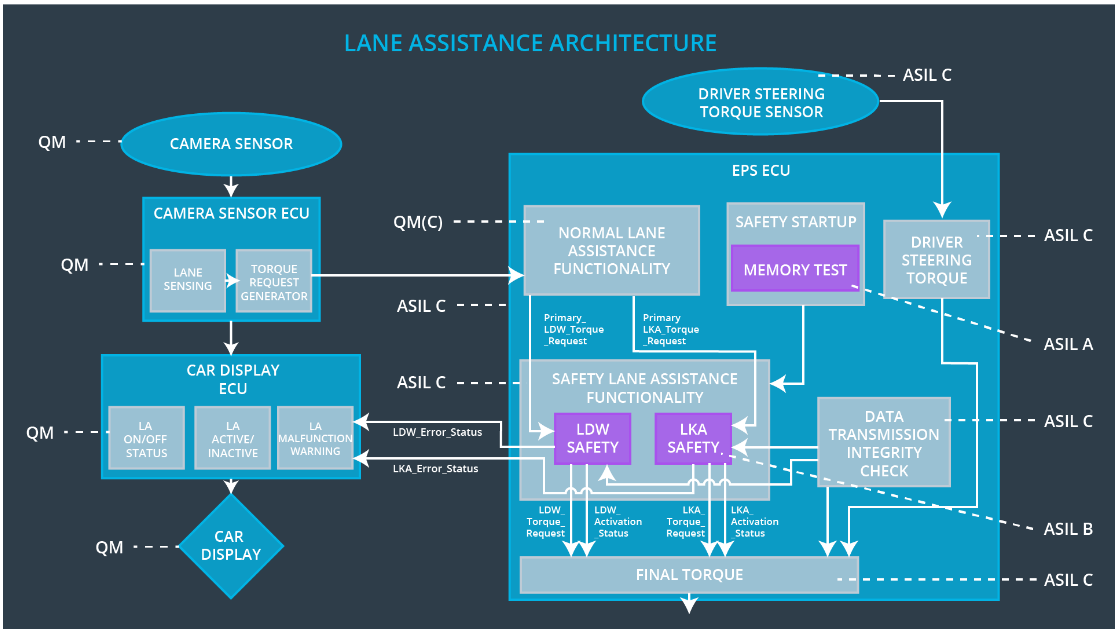

Figure 21: Refined architecture

3 Software Requirements

3.1 Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements

Table 31: Technical Safety Requirement 01

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the **'Final electronic power steering Torque'** component is below Max_Torque_Amplitude	C	50 ms	**LDW Safety** Software Block	the lane assistance item is turned off

Table 32: Software Safety Requirement

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01	The input signal Primary_LDW_Torq_Req shall be read and pre-processed to determine the torque request coming from the **Basic/Main LA Functionality** SW Component. Signal processed_LDW_Torq_Req shall be generated at the end of the processing	C	LDW_SAFETY_INPUT_PROCESSING	NA
Software Safety Requirement 01-02	In case the processed_LDW_Torq_Req signal has a value greater than Max_Torque_Amplitude_LDW (maximum allowed safe torque), the torque signal limited_LDW_Torq_Req shall be set to 0, else limited_LDW_Torq_Req shall take the value of processed_LDW_Torq_Req	C	TORQUE_LIMITER	limited_LDW_Torq_Req = 0 (Nm = Newton-meter)
Software Safety Requirement 01-03	The limited_LDW_Torq_Req shall be transformed into a signal LDW_Torq_Req which is suitable to be transmitted outside of the LDW Safety component (**LDW Safety**) to the **Final EPS Torque** component. Also see Software Safety Requirement 02-01 and Software Safety Requirement 02-02	C	LDW_SAFETY_OUTPUT_GENERATOR	**LDW_Torq_Req** = 0 (Nm)

Table 33: Technical Safety Requirement 02

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	Data Transmission Integrity Check	N/A

Table 34: Software Safety Requirement

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	Any data to be transmitted outside of the LDW Safety component (**LDW Safety**) including LDW_Torque_Req and activation_status (see Software Safety Requirement 03-02) shall be protected by an End2End(E2E) protection mechanism.	C	E2ECalc	LDW_Torq_Req = 0 (Nm)
Software Safety Requirement 02-02	The **E2E** protection protocol shall contain and attach the control data: alive counter (SQC) and CRC to the data to be transmitted	C	E2ECalc	limited_LDW_Torq_Req = 0 (Nm = Newton-meter)

Table 35: Technical Safety Requirement 03

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the **LDW** feature and the LDW_Torque_Request shall be set to zero	C	50 ms	**LDW Safety** Software Block	LDW torque output is set to zero

Table 36: Software Safety Requirement

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Each of the SW elements shall output a signal to indicate any error which is detected by the element. Error signal = error_status_input (LDW_SAFETY_INPUT_PROCESSING), error_status_torque_limiter (TORQUE_LIMITER), error_status_output_gen (LDW_SAFETY_OUTPUT_GENERATOR)	C	ALL	N/A
Software Safety Requirement 03-02	A software element shall evaluate the error status of all the other software elements and in case any 1 of them indicates an error, it shall deactivate the LDW feature (activation_status = 0)	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)
Software Safety Requirement 03-03	In case of no errors from the software elements, the status of the LDW feature shall be set to activated (activation_status = 1)	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 03-04	In case an error is detected by any of the software elements, it shall set the value of its corresponding torque to 0 so that LDW_Torq_Req is set to 0	C	ALL	LDW_Torq_Req = 0 (Nm)
Software Safety Requirement 03-05	Once the LDW functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again.	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)

Table 37: Technical Safety Requirement 04

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light C	50 ms	**LDW Safety** Software Block	LDW torque output is set to zero	

Table 38: Software Safety Requirement

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	When the LDW function is deactivated (activation_status set to 0), the activation_status shall be sent to the car displayECU.	C	LDW_SAFETY_ACTIVATION, CarDisplay ECU	N/A

Table 39: Technical Safety Requirement 05

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	ignition cycle	**Memory Test**	LDW torque output is set to zero

Table 310: Software Safety Requirement

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 05-01	A CRC verification check over the software code in the Flash memory shall be done every time the ignition is switched from off to on to check for any corruption of content.	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 05-02	Standard RAM tests to check the data bus, address bus and device integrity shall be done every time the ignition is switched from off to on (E.g.walking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations)	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 05-03	The test result of the RAM or Flash memory shall be indicated to the **LDW_Safety** component via the test_status signal	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 05-04	In case any fault is indicated via the test_status signal the INPUT_LDW_PROCESSING shall set an error on error_status_input (=1) so that the LDW functionality is deactivated and the LDWTorque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

4 Refined Architecture Diagram

The refined software architecture after specifying software safety requirements is shown on Figure 41

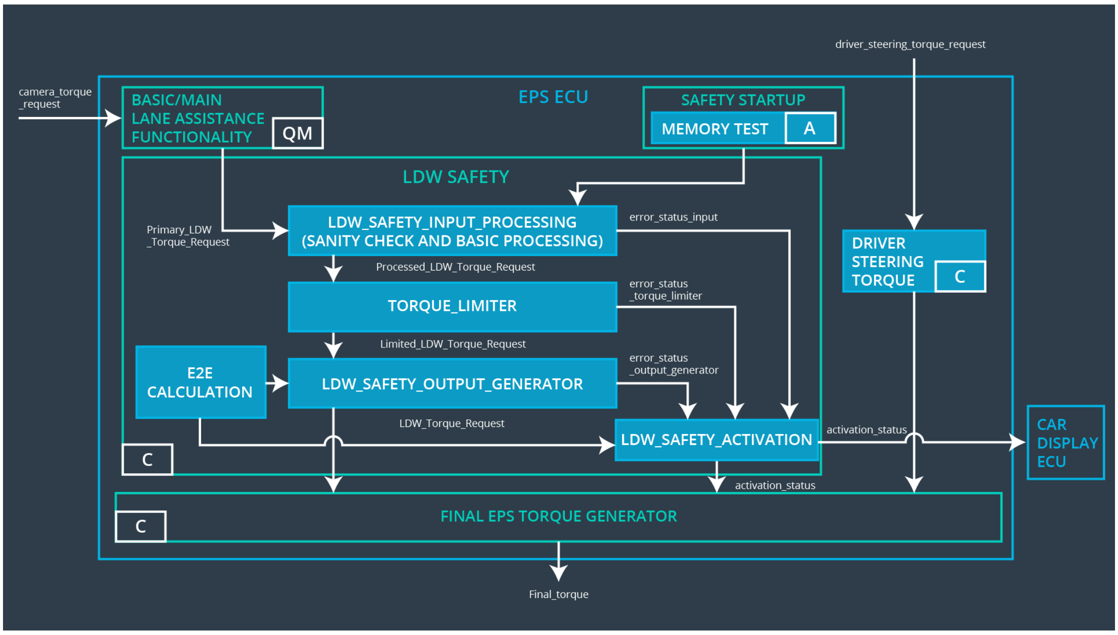

Figure 41: Refined software architecture

5 List of Abbreviations

ISO	International Organization for Standardization
ASIL	Automotive Safety Integrity Level
ECU	Electronic Control Unit
EPS	Electronic Power Steering
OEM	Original Equipment Manufacturer
LDW	Lane Departure Warning
LKA	Lane Keeping Assistance

Bibliography

[1] Organización Internacional de Normalización. *ISO 26262: Road Vehicles : Functional Safety*. ISO, 2011.